TECHNICAL NOTE		
Maple Model(s) cMT Series	**Title** Secure MQTT Connections between Maple Systems HMIs and Ignition Gateway using SSL/TLS Certificates	**TN5136**
P/N: 09075136 Rev. 00 Date: 2/24/2020		

Summary

By default, most MQTT Brokers and Clients send data unencrypted over port 1883. This Technical Note describes how to enable end-to-end encrypted connections between your Maple Systems HMIs and Inductive Automation's Ignition Gateway platform using SSL/TLS certificates.

Requirements:

Download and install the following software programs before you continue:

1. *Oracle Java version 8* or higher: https://java.com/en/download
2. *Keystore Explorer*: https://keystore-explorer.org/downloads.html
3. *MQTT.fx*: https://mqttfx.jensd.de

NOTE: You should already have ***Ignition Gateway*** with ***Cirrus Link MQTT Modules***, as well as ***EBPro*** installed on your PC prior to starting the SSL Certificate Installation process outlined below. If you do not, please see our Sparkplug B MQTT Quick-Start Guide (See: Manuals & Guides) or visit our Software Download Center to download *EBPro Full Version*, respectively.

Instructions

Create an SSL Certificate for Installation on Ignition Gateway:

Reference: This section adapted from Inductive Automation video: "How to Set Up Transport Layer Security"

Create a Java Keystore File and RootCA Certificate

NOTE: Download Keystore Explorer from keystore-explorer.org if you have not already done so.

1. Open Keystore Explorer and create a new keystore in 'JKS' format:
    A. Select: File > New > 'JKS', and click 'OK'
2. You may import a purchased certificate if you already have one or follow the instructions below to generate a self-signed certificate.
    A. Generate: Right-click on the main window (blank, white area) and select "Generate Key Pair"
    B. Select 'RSA' algorithm, key size: 2048 (bits)
    C. Leave these defaults as they are: Version 3; SHA-256 with RSA
    D. Click on the 'address book' icon next to the 'Name' field
    E. Enter a name, such as "RootCA"
    F. Fill in the Organization Unit (OU), and Organization (O) fields
        i. Example #1: OU: "IT"; O: "IA"
        ii. Example #2: OU: "Support"; O: "Maple Systems"
    G. Click OK
    H. Add Extensions: Click the green + (plus) button to add an Extension
        iii. Add Type: Basic Constraints
            1. Check the box: "Subject is a CA" and click OK to add
        iv. Add Type: Key Usage
            1. Check the boxes: "Certificate Signing" and "CRL Sign", then click OK to add
    I. Click OK to finish generating Key Pair Certificate
    J. Enter an Alias, e.g.: "RootCA", and click OK
    K. Specify a password for the keystore file. (NOTE: You will need to record this password and enter it into Ignition when you import the certificate.)
    L. Click OK. The message "Key Pair Generation Successful" should now appear.

Create and Sign a New Key Pair (Certificate) Using the RootCA

1. Right-click on the newly generated 'rootca' certificate, select Sign, and choose 'Sign New Key Pair'
    A. Select RSA, 2048-bit and click OK
    B. Add a Name
        v. Fill in the following fields:
            1. Common Name (CN), the IP address or hostname for the server
                a. Examples include: "localhost", '192.168.100.1', etc.
            2. OU (same as before)

3. O (same as before)
4. Example of Name field when finished: "CN=localhost,OU=Support,IA=MapleSystems"

C. Click OK
D. Set the Alias (leave as default), e.g.: "localhost (RootCA)"
E. Enter a password for this key pair (use the same password as before)

2. Save the keystore as 'cert.jks'
   A. Select: File > Save, enter the password, and name it 'cert.jks'
   B. Set the type to 'KeyStore Files'
   C. Click OK/Save
3. Export the Certificate Chain (.pem file) for this RootCA certificate
   A. From KeyStore Explorer, right-click on 'rootca', and select Export > Export Certificate Chain
   B. Leave these defaults as they are:
      i. Export Length: Head Only
      ii. Export Format: X.509
   C. Make sure that the 'PEM' option is checked
   D. Edit the filename and add the **.pem** extension:
      iii. Example (Original): "C:\PATH\TO\rootca.cer"
      iv. Example (Modified): "C:\PATH\TO\rootca**.pem**"
   E. Click Export. You should see the message 'Export Certificate Chain Successful'.

Ignition Gateway MQTT Distributor Settings:

1. From Ignition Gateway, MQTT Distributor Settings, click on 'enable TLS' (default port: 8883)
2. Under TLS Settings, Java Keystore File, click on 'Choose File'
3. Browse to the 'cert.jks' file saved previously, select it and click 'Open'
4. Enter the Java keystore password in the 'Keystore password' field
5. Click 'Save Changes'

Ignition Gateway MQTT Transmission Settings:

1. From the 'Servers' tab, click 'edit' to the right of the existing server
2. Change the URL from "tcp://<hostname>:1883" to "ssl://<hostname>:8883"
   a. Example: ssl://localhost:8883
3. In the TLS section > 'Certificate File Upload', click 'Choose File'
4. Browse to and select 'rootca.pem' and click 'Open'
5. Click 'Save Changes'
6. If successful, on the Servers tab, you should see '1 of 1', or '2 of 2' are now connected

Ignition Gateway MQTT Engine Settings:

1. From the 'Servers' tab, click 'edit' to the right of the existing server
2. Change the URL from "tcp://<hostname>:1883" to "ssl://<hostname>:8883"
   a. Example: ssl://localhost:8883
3. In the TLS section > 'Certificate File Upload', click 'Choose File'
4. Browse to and select 'rootca.pem' and click Open
5. Click 'Save Changes'
6. If successful, the status should say 'Connected' on the Servers tab once the change goes into effect

Installing SSL Certificates on Maple Systems HMIs

NOTE: You can use the same certificate as you installed into Ignition Gateway previously.

SSL Certificates on Maple Systems cMT HMIs, Gateways, and Servers:

1. In EBPro, from the 'IIoT/Energy' tab > 'MQTT', click on 'Settings' to open 'MQTT Server Object Properties'
2. From the 'General' tab:
    A. Change the port from 1883 to 8883
    B. Check the box for 'Authentication' and fill in the Ignition Gateway username and password
3. From the TLS/SSL tab:
    A. Check 'Enable' and check 'Server verification'
    B. Uncheck "Server name must match certificate's information"
    C. Click 'Import...', browse to and select the 'rootca.pem' file, and click Open
    D. Click OK, then click Exit on the main MQTT Options window

Test the SSL encryption using Online or Offline Simulation mode in EBPro

- If the (simulated) HMI cannot connect to the server, double-check the username and password entered on the General tab and try again.
- Else, if unable to connect, check the Ignition Gateway logs for additional error messages.
- If your EBPro installation is on a separate PC than your Ignition Gateway server, you may need to open port 8883 on either or both PCs in order for communication between the two devices to be established.
    - See our Sparkplug B MQTT Quick-Start Guide (See: Manuals & Guides) for more information on networking and firewall settings.
- Once you are able to establish a secure connection using Simulation mode in EBPro, you may download the project to your HMI.

NOTE: Visit our Sample Projects page in order to download a free copy of our *Sparkplug B MQTT Sample Project*. You can use this for testing purposes or adapt it for your own application.

Installing SSL Certificates in Third-Party MQTT.fx Client Software

MQTT.fx is a free, open-source MQTT Client with support for Sparkplug B via built-in 'Sparkplug Decoder'.

1. Download and install MQTT.fx if you have not already done so.
2. Create a new connection (click on the ‘Gear’ icon).
3. Fill in the Profile Name (e.g. “Ignition SSL”).
    A. Leave these defaults as they are:
        1. Profile Type: MQTT Broker
        2. Client ID: MQTT_FX_Client
    B. Set the Broker IP Address to the Ignition Gateway IP address
    C. Set Broker Port to 8883
4. Leave the defaults as they are on the ‘General’ tab
5. On ‘User Credentials’ tab: Fill in the Username and Password as used in Ignition Gateway
6. On the ‘SSL/TLS’ tab:
    A. Check 'Enable SSL/TLS', protocol TLSv1.2
    B. Select 'CA certificate file'
    C. To the right of the 'CA Certificate File' name field, click on the 'Open' button [...]
    D. Browse to and select the 'rootca.pem' file, and click Open
    E. Click OK
7. Click Connect
    A. If successful, you should see the circle icon in the top-right corner of the program turn Green
    B. Next, the lock icon should become 'locked', indicating the connection has been secured using SSL
8. From the Subscribe tab, subscribe to all topics on the Ignition Gateway:
    A. Enter a "#" and click 'Subscribe'
9. In the lower-right hand corner of the program, find the “Payload decoded by” drop-down menu:
    A. Select ‘**Sparkplug Decoder**’ to properly decode messages published by Ignition
10. Generate data from your HMI (or from a Simulation in EBPro) and observe the messages being published by the Ignition Broker. These will be listed and displayed one at a time within MQTT.fx.

OPTIONAL: Disable Unencrypted MQTT Connections in Ignition

NOTE: To ensure the security of your process data sent via MQTT, it is recommended that you disable all unencrypted MQTT connections after setting up SSL Encryption.

Follow the steps below to disable unencrypted MQTT connections (port: 1883) to your Ignition Gateway.

1. From MQTT Distributor Settings > non-TLS Settings, uncheck the following option:
    A. Uncheck: “Enable plain TCP connections for the MQTT Server”
2. Click ‘Save Changes’.
3. Your Ignition Gateway will now no longer accept unencrypted TCP connections.